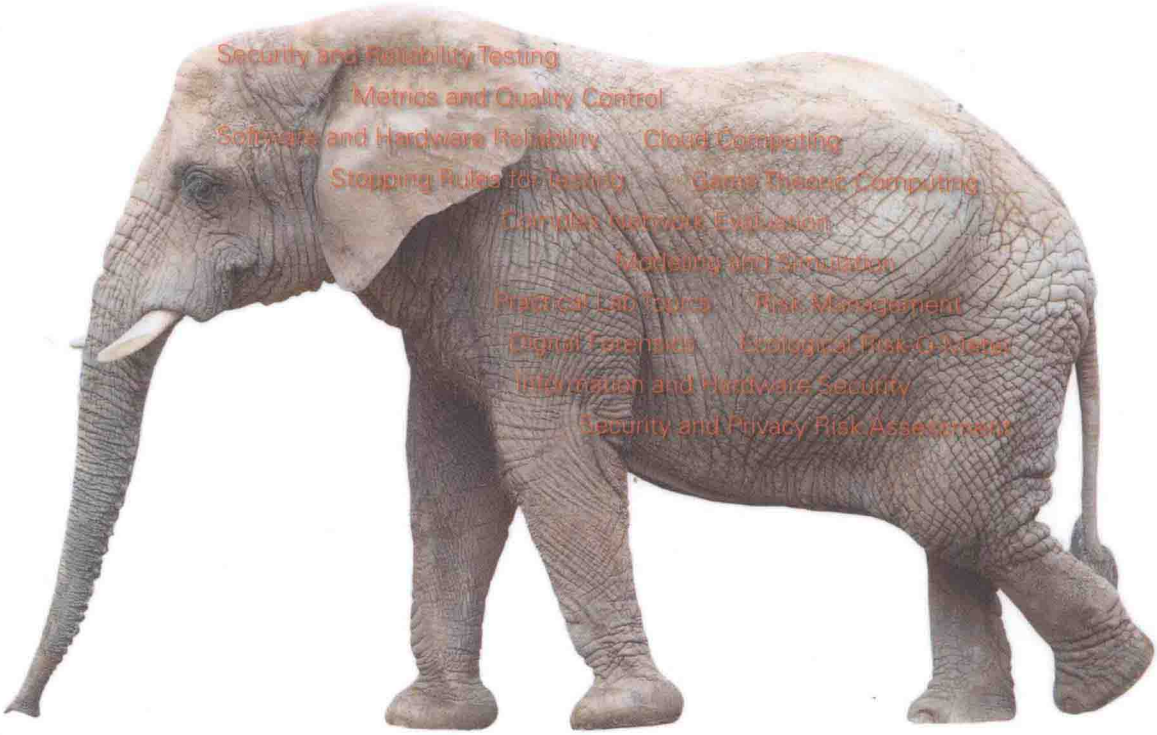
CYBER-RISK INFORMATICS

Engineering Evaluation with Data Science



Mehmet Sahinoglu

with website

WILEY

CYBER-RISK INFORMATICS

Engineering Evaluation with Data Science

MEHMET SAHINOGLU, PH.D.
Auburn University at Montgomery

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada

Library of Congress Cataloging-in-Publication Data

Names: Sahinoglu, Mehmet, 1951– author.
Title: Cyber-risk informatics : engineering evaluation with data science / Mehmet Sahinoglu.
Description: Hoboken, New Jersey : John Wiley & Sons, 2016. | Includes bibliographical references and index. | Description based on print version record and CIP data provided by publisher; resource not viewed.
Identifiers: LCCN 2015036259 (print) | LCCN 2015032749 (ebook) | ISBN 9781119087526 (Adobe PDF) | ISBN 9781119087533 (ePub) | ISBN 9781119087519 (cloth)
Subjects: LCSH: Cyber intelligence (Computer security) | Computer systems–Reliability. | Computer software–Reliability. | Computer networks–Security measures–Data processing. | Risk assessment–Statistical methods.
Classification: LCC QA76.9.A25 (print) | LCC QA76.9.A25 S2497 2016 (ebook) | DDC 005.8–dc23
LC record available at http://lccn.loc.gov/2015036259

Set in 10/12pt Times by SPi Global, Pondicherry, India

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

ABOUT THE COVER

The multifaceted nature of network security reminds one of the ancient fable, the parable of *The Blind Men and the Elephant*, where the blind men (or security risk researchers today) are touching the elephant (or network security) to understand what it really is or isn't, because they have never encountered an elephant before. One man touches the elephant's tusk, and the other its side, while another touches its tail and yet another its trunk. When they reunite to discuss their findings, they cannot agree what the elephant looks like; such as one thought the trunk was a snake, and the other imagined a tree branch, and so it goes. Much the same happens when it comes to cyber-risk assessment and management. Network security is such a complex, multifaceted topic that cyber-risk specialists are like the veritable blind men grasping at parts and unable to understand the elephant completely. This book's intent is to provide a timely remedy to that symbolic "elephantine" metaphor's puzzle by providing a holistic-theoretical and philosophical as well as practical, user-friendly and useful, and application-oriented within a well-grounded holistic approach to network security risk assessment, such that those *blind men* will no longer be so unfamiliar with the *elephant*! The universal message here is not seeking total "security" (a perfect knowledge of the elephant by seeing it, never to happen for the blind men), however focusing on managing the "insecurity" (understanding the elephant in the best manner that the blind men could), which is what this pioneering textbook is all about.

PROLOGUE

"A little neglect may breed great mischief...
For want of nail, the shoe was lost;
For want of a shoe, the horse was lost;
And for want of a horse, the rider was lost."

Benjamin Franklin, Poor Richard's Almanac 1758

"A little lack of countermeasure may breed great breach...
For want of firewall, the software was lost;
For want of software, the hardware was lost;
And for want of hardware, the user was lost."

Mehmet Sahinoglu, Cyber-Risk Informatics 2016

REVIEWS

The *Cyber-Risk Informatics* is a sequel to Dr. Sahinoglu's earlier Wiley text of 2007 and is a reinforcement of his popularized risk metric approach to assessing and managing security and reliability of cyber components and networks at large. His Cyber-Risk assurance modeling, employing math statistically sound metric approaches, from Healthcare to Cloud Computing to name a few themes that he has implemented is not to be encountered in today's many case study-based textbooks. I certainly take pride in writing a new foreword this time 8 full years later for his follow-up as I was pleased to personally recommend back in 2011 to prepare a new manuscript to incorporate all of his new findings and journal publications. The inaction of not creating this text otherwise would have left a serious void and waste of resources to reach our new generation of risk (fire) fighters to quench the widely prevalent network (forest) breaches (arsons) as the metaphor goes, if you will.

It is my distinct pleasure to highly recommend this book of multi- and transdisciplinary nature equipped with numerical methods and directly related to software application provided for the readers and students as a gluing medium to synergize all the necessary components of research from Testing to Simulation and from Security Assessment to Cloud Computing and hands-on lab practices. His goal to emphasize the strong link between the academic and corporate worlds that complement one another is well justified. I strongly recommend anyone eager to learn new depths in Cyber-Risk modeling to visit this museum of knowledge that will become a scientific classic to refer to in the decades ahead.

In Memoriam: The academic world with great sadness has lost Professor CV Ramamoorthy on March 9, 2016 to eternity at 90; however his spectacular deeds and unforgettable selfless enlightenments of all scholars around the world will never get lost, and his ever-smiling countenance full of wisdom will always be remembered endlessly at every occasion. A good man and gentleman, who helped many when they were in down

times, has proudly made his journey. He was a gentle guide and kind mentor to countless and will be dearly missed. May he rest in peace!

Posthumously To: Dearest Professor Ramamoorthy, This book would have been in your masterful palms adorned and enriched with your natural, humbling observance had you in good health prevailed since the book's prompt delivery was arranged to be sent to you by WILEY. You still will receive it. I would be remiss if I did not quote your timeless and wonderfully crafted e-mail related to the essence of a textbook you encouraged me to compose when you said this project was a must-do. Forever Gratefully!

Dear Prof. Mehmet,
Wonderful information. The topic you are discussing is most important and timely. Please compose an excellent text into an easy to follow sequence of the critical ideas in your presentation—for the layman, to a graduate engineer, and a practicing entrepreneur or financial banker. As I mentioned before, you have the God-given talent in conveying in a very comprehensible form the complex ideas people often find difficult to simplify. I am forwarding this recommendation to John Wiley publisher, Dr. Brett Kurzman of John Wiley to entice you to develop this project. Warmest Regards. Sincerely / RAM

C. V. Ramamoorthy, M.S./Ph.D., Harvard University in EE and Applied Math (Computer Science) Distinguished Professor (Emeritus) of Computer Sciences and Electrical Engineering at the University of California at Berkeley, California. His awards are not limited to IEEE Life Fellow, SDPS Fellow and SR Research Fellow of the ICC Institute at the University of Texas, Austin; Honorary Doctorate in Taiwan and many universities around the world; Editor-in-Chief of *IEEE Transactions on Software Engineering* and *International Journal of Software Engineering and Artificial Intelligence* and *IEEE Transactions on Knowledge and Data Engineering*; Coeditor-in-Chief of the *International Journal of Systems Integration* and of the *Journal of the Society of Design and Process Science*; Distinguished Scholar Award, Society for Design & Process Science, 1995; IEEE Richard E. Merwin Award, 1993; IEEE Computer Society Meritorious Service Award, 1991; IEEE Computer Society Taylor Booth Award, 1990; IEEE Computer Society Outstanding Award, 1987; IEEE Centennial Medal, 1984; Fellow, IEEE, 1978; IEEE Computer Society, Special Education Award, 1978; IEEE Computer Society, Honor Roll Award, 1974; Admiral Grace Hopper Chair, Naval Postgraduate School and others.

The critical status of cybersecurity in today's connected world is self-evident from countless unwanted security breaches in all walks of life. The *Cyber-Risk Informatics* has many interesting discussions and illustrative examples that will present students and other researchers an overview to understand the importance of this area. Furthermore, this book, in addition to examples, presents several computational and intellectual challenges to students and other researchers in this area. The new text on cyber assurance modeling proceeds with a good foundation in mathematics and statistics and culminates to game-theoretic risk computing (including the sensory networks), as well as simulation-based best practices and continues with the popular topic, such as Cloud Computing, in terms of its performance characteristics. This text finally offers the students and researchers a chance to learn enough about the hands-on lab practices to help land a decent cybersecurity job. These building blocks click well with synergy while carefully executed through plenty of examples and screenshots. It is a useful reference text for students and researchers

taking courses in search for cybersecurity metrics and risk management methods given the lack of technical resources in this area.

S. S. Iyengar, Ph.D., Director and Ryder Professor, Department of Computer Science FIU School of Computing and Information Sciences, Miami, FL. His awards are not limited to IEEE Fellow, ACM Fellow, AAAS Fellow, and National Academy of Inventors Fellow; Recipient of Florida Innovation Award; The Association of Scientists and Developers and Faculty Award (India); Distinguished Service Award (LSU); Distinguished Research Award (China); IEEE Computer Society Technical Achievement Award; IEEE Computer Society Meritorious Award; IEEE Computer Society Golden Core Membership; LSU Prestigious Distinguished Research Master Award; IEEE Distinguished Visitor, NASA Faculty Fellow; Editor to 16 IEEE and other journals; authored 20 books from sensors to robotics with 5 patents and numerous grants.

In my daily dealings as a director of a cybersecurity center of national importance and as an academician, I have felt the need for a book that gives me foundations and tools to deal with important issues on risk assessment in cybersecurity. Not only I but my many peers across the country have felt the void of a pedagogical resource that combines building blocks of quantitative concepts and practice of risk assessment. This much needed book fills a void in the cybersecurity field. The field of cybersecurity has advanced at a very rapid pace, but the theory and pedagogical components have not kept pace with this advance. This is perhaps the first book that first gives the fundamentals of risk assessment, much needed statistical foundations, network principles, reliability, game-theoretic foundations, etc. and presents it an easy-to-understand manner without compromising the rigor of the field. The book will be very useful to layman and practitioners in the cybersecurity arena, especially in regard to the hands-on lab exercises, as in Chapter 10 and full Java-assisted applets in the Cyber-Risk Solver website with a solution set.

I know that this book will be on my desk within easy reach. I can find no other person better qualified than Professor Mehmet Sahinoglu to address the very important areas of quantitative risk assessment. Professor Sahinoglu brings the best of his academic expertise and 35 years of experience in the field to present a unique balance of theory, practice, and research in this book. The pedagogical components including examples and lab exercises make this book unique and exemplary.

Vir V. Phoha, Ph.D., formerly Director of Center for Secure Cyberspace, College of Engineering, Louisiana Tech University, Ruston, LA; currently Professor of Electrical Engineering and Computer Science, L.C. Smith College of Engineering and Computer Science, Syracuse University, Syracuse, NY.

This may be the first book of its kind in a long time—one that brings real engineering and science back into the world of Cyber-Risk assessments. One of the growing challenges in the world of security today is simply to arrive at a concrete definition of risk. There are literally thousands of books written on or related to the subject of risk in the cybersecurity world. However, finding a book that describes risk in quantitative terms is nearly impossible. The modern practice of determining Cyber-Risk is instead left to the philosophical whims of qualitative deductions and long lists of gadgets and software that will surely make you cyber secure. In a time when computing power is at an all-time high, we find ourselves

facing a dearth of knowledge with regard to understanding how much risk we are actually exposed to in our systems. So the question remains, "Does anybody really know what Cyber-Risks we are taking?" Certainly we will never answer that question if we continue merrily down the path of nonquantitative or quasiquantitative methods we are currently pursuing. However, we will also never be able to sleep at night actually knowing the amount of risk we are accepting in our modern and interconnected systems and whether some morning we will all wake up to a world gone mad because of a colossal cyber-attack.

Therefore, it makes sense to once again make an effort to move the Cyber-Risk assessment process back into the world of quantitative methods and concrete conclusions so that we can sleep without anxiety for the morning. Putting the science and rigor back into Cyber-Risk assessments is a great place to start and will directly influence the cyber awareness of both our military and corporate enterprises. Dr. Sahinoglu makes an excellent start at doing just that. Let the quantitative versus qualitative wars begin—again.

Joel Junker, Lt. Col. USAF (Ret.), CISSP, Vice President of Security Systems at DSD Laboratories.

This timely, must-have book provides a rigorous scientific modeling approach for conducting metrics-based quantitative risk assessments in the face of ever-increasing sophistication and ubiquity of cybersecurity threats. This collection of invaluable, thoroughly vetted work not only provides the building blocks for a solid academic foundation that helps students to be better prepared to enter the cybersecurity workforce but also provides a relevant, practical reference for the application of metrics-based quantitative risk assessments in the industry sector. The role of scientific-based quantitative cybersecurity risk assessments in the decision-making process cannot be overstated. Assuredly, while uncertainty exists in any risk assessment process attempting to evaluate a wide breadth of variables associated with threats and the vulnerabilities exposed to those threats, Dr. Sahinoglu's building blocks clearly describe how those uncertainties can be drastically reduced via a disciplined framework that can increase speed, reliability, and accuracy in a cost-effective manner. In an environment where speed, accuracy, and reliability are crucial in determining the risks associated with the vulnerabilities and respective countermeasures, it is crucial for industry to have the tools at their side to counter the threats. Dr. Sahinoglu's book does just that.

Anthony Buenger, Lt. Col. USAF (Ret.), CISSP, Chief, Cybersecurity Assurance Division, Air Force Life Cycle Management Center, Maxwell AFB, Montgomery, AL.

Prof. Sahinoglu has succeeded in authoring a groundbreaking and outstanding book that manages to combine years of fruitful expertise with the explanatory power of a well-structured text. This book stands out as a magnificent source of technical information, artistically visualized and depicted, backed up with a solid structure from beginning to end, promising anyone in the field, whether student, scholar, or analyst, a well-thought-out reading experience that comprehensively addresses every topic required in the cybersecurity field. On examining the book for the first time, we immediately decided to open up courses and workshops in August 2014 at Middle East Technical University (METU) in Ankara, Turkey, to study the topics in detail, so that our staff and students in METU's Cyber Security graduate program and METU Cyber Defense and Security Center (CyDeS) would benefit from his innovative research.

In most courses and textbooks, risk analysis has been approached from a management perspective, which is not the case in this book, which takes, rather aptly, a quantitative matrix-based approach with much concreteness and succinctness in addressing every possible factor involved in the field. As we are all familiar, cybersecurity has a self-evident interdisciplinary nature, which is reflected quite efficiently and clearly in the content and style of this book. Prof. Sahinoglu has internalized the interdisciplinary nature of the field in its all comprehensiveness and presents it to readers together with the most up-to-date information. Without any doubt, the book is destined to fill an immense gap in the cybersecurity field, with its technical resources, quantitative methods, educational extras, structure, and approach.

I am delighted to predict that the book will turn into a reference book for all students as well as the scholars at the METU Informatics Institute Cyber Security graduate program.

Nazife Baykal, Ph.D., Professor and Director of the Informatics Institute, Head of the Cyber Security Department of Informatics Institute of Middle East Technical University (METU), Ankara, Turkey; Director of METU Cyber Defense and Security Center (CyDeS); currently conducting research on Cybersecurity, Health, and Medical Informatics; and author of "Computer Networks."

This is a unique book that covers several related issues in Computer Systems like security, risk management, quality control, and reliability. Since Prof. Sahinoglu has contributed to these topics both as a teacher and a researcher, he manages to convey concepts clearly, precisely, and passionately. One of the main contributions is the quantitative approaches based on metrics analysis. This book can be useful for reference, for research, or as a textbook for advanced graduate or postgraduate courses. It could also inspire new postgraduate or Ph.D. courses on those topics.

Nestor R. Barraza, Ph.D. Professor of Computer Science at the Department of Engineering, Universidad Nacional de Tres de Febrero. He is also with the Electronics Department at the School of Engineering, University of Buenos Aires, Argentina.

In this vastly connected and rapidly moving cyber world, our ability to counter the ever-present security risks has not been able to stem the growing tide of actual cyber breaches. I am very happy to see finally a comprehensive treatment of Cyber-Risks, as contained in this readable book. Dr. Sahinoglu's work over the last 20 years has been focused on ensuring that computing devices are secure enough to be worthy of the trust of users. He has made significant contributions in this brand new area of research. One of his major earlier contributions is the Sahinoglu–Libby probability distribution model, which characterizes the behavior of failure patterns in components/networks and software systems; a set of optimal algorithm-driven stopping rules for terminating software testing; and the concept of security meters to set protective measures for certain required system security levels.

With the Sahinoglu–Libby model as a basis, Dr. Sahinoglu devised a number of surprisingly simple, practical, and yet vigorous data-analytic approaches for the analysis and prioritization of security and privacy risks. His work addresses a long-standing gap in cybersecurity—the ability to accurately measure the risk of compromises, as well as to provide discrete financial impacts of various security and privacy events while a complex system is in operation. By utilizing a multitude of quantitative modeling and estimation techniques, Dr. Sahinoglu provides the needed tools for security analysts/engineers to

generate a broad array of scenarios for simulation and analysis. Moreover, his techniques can be utilized across a variety of security disciplines and domains.

I highly recommend this readable book to all people who are involved in the area of cyber-security. Typical to Dr. Sahinoglu's approach, this book, utilizing a data analytical approach, provides comprehensive coverage of the latest applied and quantitative metrics-oriented topics in Security and Reliability Modeling for risk assessment. It is indeed a very impressive work of passion, knowledge, and hard work. It is my expectation that the impact of this well-written book on academia, industry, and our highly connected society will increase greatly in the years to come as new generations of cyber-security analysts, engineers, and managers are being educated in this foundational work.

Raymond T. Yeh is a retired Professor of Computer Science and entrepreneur. He is an IEEE Life Fellow. He was the CDC Distinguished Professor at the University of Minnesota and the Chair of the Department of Computer Science at both the University of Texas at Austin and the University of Maryland at College Park. He was also the founding Editor-in-Chief of *IEEE Transactions on Software Engineering* and founder of *IEEE International Conference on Software Engineering* (ICSE).

This is a unique book on trustworthy computing that continues the series of the books on this timely popular area created by Dr. Sahinoglu. In short, the book can be characterized as the encyclopedia of the state-of-the-art cyber risk techniques and metrics based on the author's approach. Actually the book is one of the world's first and probably the widest scope books on quantitative assessment of cyber security and cyber risk issues. The scope of the book is uniquely large. In particular, it covers quantitative aspects for traditional MTBF and MTTR reliability models; quantitative assessment of network security and risk; game-theoretic approach to cyber risk assessment; modeling and simulation techniques in cyber risk assessment, and many other cutting-edge topics. The most interesting and innovative from my viewpoint is the chapter on quantitative assessment of cyber risk in cloud computing. This chapter is my favorite and is very close to my heart as a cloud computing expert.

Another very attractive aspect of the book is a unique combination of original theoretic methods for quantitative cyber risk assessment with lots of real-life examples of the tasks to be solved by those methods, lots of exercises, hand-on labs, tables and illustrations on each important concepts, methods and topics covered in the book. I do think the book is necessary for each IT student and expert, not just to read, but to very carefully study to grasp this innovative material. The book can be used for any kind of trustworthy computing classes at any university elsewhere, and also for self-education. The book positions the author Dr. Sahinoglu as a worldwide classicist in IT in general and trustworthy computing in particular.

Vladimir O. Safonov is a Professor of Computer Science at St. Petersburg University, one of the leading IT experts in Russia as a Corresponding Member of the Russian Academy of Natural Sciences and a Renowned Contributor to Science and Education at this Academy. His areas of expertise are: cloud computing, trustworthy computing, aspect-oriented programming, knowledge management, programming languages and compiler development, Java and .NET technologies, operating systems, parallel programming, software architectures. He is the author of 17 books, including three Wiley books: "Using aspect-oriented programming for trustworthy software development" (2008), "Trustworthy Compilers" (2010), and "Trustworthy Cloud Computing" (2016), and the author of over 190 articles.

PREFACE

This book is authored out of a dire necessity of merely not finding all SECURITY related core and internship topics in a textbook proper while teaching an advanced cybersecurity graduate course, for example, CSIS 6013, "Network Security and Reliability—Quantitative Metrics," in a recently new graduate degree program founded by the author and accredited in December 2010. The book also relates to CSIS 6912, "Internship: Supervised Practicum with Cyber-Industry Experience," and CSIS 6952, "Security Policy Seminar." See www.aum.edu/csis. These courses have traditionally covered various topics in Cyber-Risk Computing. However, there is no one book that covers the newest applied and quantitative metrics-oriented topics in Security and Reliability Modeling. This book utilizes a data analytical or data scientific approach rather than heuristical and ad hoc methods that most authors employ through individual case studies without scientific modeling that should apply to all cases. Data science is the extraction of knowledge from data where data scientific techniques affect research in many domains, including the biological sciences, medical informatics, healthcare, social sciences, and the humanities. From the business perspective, data science is an integral part of competitive intelligence, a newly emerging field that encompasses a number of activities, such as data mining and data analysis. Data scientists investigate complex problems through expertise in disciplines within the fields of mathematics, statistics, and computer science. Graduate-level exposure as well as a senior class level at an accredited university is a preferable background for the study of this topic. It is anticipated that the audience will be advanced undergraduate and beginning graduate students in the general area of Cybersecurity, Information Technology (a topic that also covers the practitioners), Applied/Computational Statistics, Computer Science/Engineering, or Industrial Engineering Departments for having already been exposed to courses in Security, Reliability, or Dependability. The role of a Cyber-Risk Informatics program graduate is fundamentally similar to an IT graduate, though more possessed with a keen and all-purpose motivation on multifaceted Risk and its repercussions as to how to assess and

mitigate the common foe. Cyber-risk Informatics is strictly multi- and transdisciplinary in nature. For example, twenty such roles can be itemized for a Cyber-risk Informatics Scientist and/or Engineer who researches and/or builds as follows:

- Demonstrate an understanding of the technical, management, and policy aspects of cyber systems and information security.
- Identify and respond to information security challenges in distributed and embedded systems.
- Recognize the impact of security issues related to software engineering on distributed information systems.
- Assess information security risks faced by an organization and develop a response plan.
- Demonstrate an understanding of technological and human engineering problems linked to security risks.
- Assess the impact of information security policies and market developments on complex systems and organizational objectives.
- Evaluate and recommend technological tools and protocols to protect against risks.
- Mitigate system vulnerabilities and restore compromised services.
- Manage the development, acquisition, and evolution of a secure information network.
- Construct secure networked and distributed computer systems.
- Troubleshoot large-scale information networks and distributed systems.
- Establish requirements for complex security applications and translate these requirements into design architecture.
- Integrate the use of encryption technology in nonsecure and nonprivate computers and systems.
- Design and conduct research in the area of cyber systems and information security.
- Critically evaluate and apply research and reports of threats to computers and cyber systems.
- Discuss the importance of lifelong learning and professional development in information security disciplines.
- Develop an ability to apply knowledge of statistical computing and mathematics specific to the discipline.
- Develop an understanding of professional, ethical, legal, security, and social issues and responsibilities needed to communicate effectively with a range of audiences and to engage in continuing professional development.
- Develop an ability to identify and analyze user needs and take them into account in the selection, creation, evaluation, and administration of risk-conscious computer-based systems so as to effectively integrate IT-based solutions into the user environment.
- Develop understanding of industry best practices and standards in Cyber-Risk Informatics area and their application.

Primary audience (the people who will find the book a must-have, such as in academia at a graduate or senior college level and similarly CS/MIS/CIS/Cybersecurity researchers):

This is an original and one-of-a-kind metrics approach, based on the author's teaching and research expertise and his previously published books and papers. The author methodically builds from a common understanding based on previous class-tested works to introduce the reader to the current and newly innovative approaches to address the maliciously-by-human-created (rather than by-chance-occurring) threat and related cost-effective management to mitigate such risk. The approach is rational and logical and provides clear entry points for readers of varying skill sets and backgrounds. All students and practitioners (including engineers, applied statisticians, and computer analysts) in the field of Risk Assessment and Management regarding Security and Reliability Modeling are now seriously examining this new-century's popular and notorious topic due to an urgent need to learn more about the common enemy: Indefatigable Risk. How to assess it quantitatively (not only using adjectives) and how to most economically alleviate and assess/manage the risk as the trillion-dollar question as self-evident from the wasted billions of dollars caused by hacking and breach of privacy at an increasing rate? The enriched Java applets provided by the author at the book's website (www.areslimited.com) will enable the reader analyst to utilize the course-related problems with less little effort than normally required. This book aims to fill a gap in current literature by developing a golden thread from classic (and merely descriptive) approaches to risk analysis, and to more demanding rigorous quantitative approaches, and supplying the reader with common implementations and use cases. The organization of the book is planned in mastery, quickly developing a background and base of knowledge before moving into new areas of research and implementation and hands-on lab. The book offers a logical outline that provides to a broad range of readers the ability to pick up anywhere based on their level of competency and working knowledge of similar subject matters. This book aims to fill a significant gap in both lay professional and research texts in the subject area. That is, because of the way the book is developed from background to innovative research, it should reach a much broader target market than traditional academic-only texts. A major strength is that the book was developed while teaching advanced undergraduate and graduate courses by the author. This means the need is perceived from real in-class experience. The author has spent a considerable research effort on this matter evident from his peer-reviewed research and extended writings including a 2007 textbook by John Wiley and Sons, Inc. This book fills a significant gap in titles available vis-à-vis quantitative approaches to risk management and provides a fair mix of theory and application. The book also reserves the flexibility and quality of an online distant educational tool for all continents.

Secondary audience (the people who will find this book a nice-to-have support material such as industrial risk managers in multiple industry verticals dealing with complex graphs and models):

Interested and curious readers belong to this category such as positive scientists and practicing engineers on risk, from the viewpoints of security and risk-related topics or both, such as those from DHS, Mining, Ecology, Safety, etc. whose topics are covered intermittently in the book's wide-ranging applications. The book is robust and, compared to other books on the market, relatively complete given the breadth of content covered. It fills a significant gap in current texts by providing a "one-stop shop" when evaluating

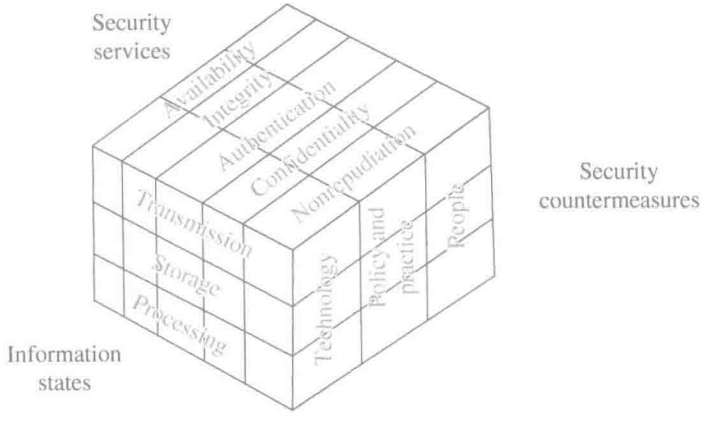


FIGURE 0.1 A summary of concepts as placed on the faces of a die. (Reprinted with courtesy of ACM from "IT 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology.")

strengths and weaknesses in existing approaches to risk assessment and cost management while offering innovative and viable ways to quantitative evaluation. Providing the reader with access to the reliability/security modeling and simulation tools outlined in the text is primary (source code, compiled code, or web-accessible mod/sim tool) and is a noted advantage of the book with plenty of applications.

Why this book is original for academia and cyber industry?

It is anticipated that the followers of this book will be advanced undergraduate (junior/senior) and beginning graduate students in the general area of Cybersecurity, Information Technology (which also covers the practitioners), Applied/Computational Statistics, Computer Science/Engineering, and Industrial Engineering Departments who have been exposed to Security, Reliability or Dependability curriculum. For related programs, one realizes the importance of this book's topics for Computer Assurance or Trustworthiness as well. See http://www.acm.org/education/curricula-recommendations of the Association for Computing Machinery (ACM), which breaks down Computer Science, Computer Engineering, Information Systems, Information Technology, and Software Engineering. See Figure 0.1.

Also p. 27 of http://www.acm.org//education/curricula/IT2008%20Curriculum.pdf explains the draft *Computing Curricula 2008 and Onwards*, which details below the listed concentrations in line with the proposed book's topics for the general topic of Information Technology. Also see Appendix B on pages 129–130 in the same link for descriptions of the IT Fundamentals. The following are the related topics that this book mostly examines related to the ACM curricula studies in the same reference.

IAS, Information Assurance and Security (17 core hours)

1. IAS. Fundamental Aspects (3)
2. IAS. Operational Issues (3)
3. IAS. Policy (3)
4. IAS. Attacks (2)

5. IAS. Security Domains (2)
6. IAS. Forensics (1)
7. IAS. Information States (1)
8. IAS. Security Services (1)
9. IAS. Threat Analysis Model (1)

MS. Math and Statistics for IT (38 core hours)
MS. Basic Logic (10)
MS. Discrete Probability (6)
MS. Functions, Relations, and Sets (6)
MS. Hypothesis Testing (5)
MS. Sampling and Descriptive Statistics (5)
MS. Graphs and Trees (4)
MS. Application of Math & Statistics to IT (2)

The primary purpose therefore is to inform senior undergraduate or beginning graduate students about the newest advances in the second decade of a new century on *Security and Reliability Modeling* with an index-based quantitative approach, in contrast to often encountered verbal or qualitative or subjective case histories that may become obsolete in the next few years when new cases arise. Rather than what this book is about, what is this book not about? This book is not a collection of already available routine chapters that can be found in a multitude of books, therefore avoiding repetitious and readily available encyclopedic information. It is objective and data driven and provides a real-world engagement for practicing statisticians and applied engineers. That said, a healthy comparison with earlier cited methods about how one reaches the new frontiers will be examined. Therefore, there will be a minimal duplication of review text material already encountered, such as the statistical probability distributions, and their simulations in compact formats, or reliability models, unless one or two of which are in close association with the innovative topics presented.

There will be a website (www.areslimited.com) that will enable the reader or student to work with hands-on-experience projects, generated in the past decade with a painstaking, fine-tuned effort and high precision detail. Additionally there are very few books that cover the quantitative metrics-oriented Security and Risk-related topics. This new proposition however is unique as it is purely statistical data oriented, employing computationally intensive techniques such as Monte Carlo simulation, in prestigious journals on assurance sciences. It is also expected that practicing engineers will be able to use the book to benefit their own case studies, examples, and projects by using the meticulously prepared project-website that accompanies the book. A detailed solutions manual and Power point slides will be prepared for both the instructors and students' use at www.wiley.com/go/sahinoglu/informatics. Therefore, there will be an "Exercise Solution Manual", "Power point slides", and JAVA-ready-to-go applications at www.areslimited.com that are different than what other textbooks provide. Moreover, the author has a well-thought-out approach for introducing the topics in the book. This is not a verbal casebook as frequently observed in textbooks that cite "what and how" in a case study with next to none of Engineering and data-scientific modelling.

The book contains a lot of information in the area of quantitative risk assessment that simply does not appear in other books that display none other than scant touches sporadically. Since the topics covered in this book are relatively new, there is much originality contained in this vivid and dynamic book. Many of the topics within the book are cutting-edge research and have applications currently being developed (or already being implemented). A thorough screening of the book media on the web clarified that no other work goes into details as such, other than case histories and general mathematical or statistical theorems without any ready-to-use applications presented before you to be used immediately. In other words, the vast majority of books available on the market do not allow self-inspired creativity because of a lack of scalability, versatility, and programmability into different disciplines. That is, these case-history specialized and one-way-street books lack interdisciplinary patterns. The author believes that the introduction of Chapter 1 needs to be comprehensive but not exhaustive in its review for the book, since there is a good amount of coverage of these standard topics elsewhere in the literature. However through the following chapters, there are many advanced areas discussed throughout the book, requiring more than a hand calculator as in most College Business and Science programs. This aspect should rather be regarded a strength to capture many new emerging concepts and ideas and therefore provides an author-facilitated web access to implement these ideas. The author believes a Cybersecurity curriculum (rather, lack of it in the light of the current fast-paced *cyber cold wars* between the leading cyber powers) is a fast-growing area with many changes and new advancements. The concepts described in this book are relevant and important for individuals interested in computer security and quantitative risk assessment.

Would any supplementary material, for example, a supporting website, be necessary or useful?

Yes, there will be a website to which readers are expected have access so that they could run the applications discussed in the book to solve homework and project problems (www.areslimited.com). It is important for the readers to be able to apply the methodology in the book to really understand the concepts. In addition, the author has the reader follow up with many examples throughout the book as tested while decade-long teaching this material from his notes and a similar-purpose book he published nine years earlier. The book-specific website, www.areslimited.com also will usefully provide the data sets in the examples and any relevant exercises in the "Exercise Solution Manual". To recap, competitive and comparative publications so far in the market generally:

- Approach the problem from roughly estimating with high degrees of error (e.g., qualitative inputs are mapped as quantitative values effectively creating a qualitative model with error rates based on human intuition and judgment call, not supported by statistical sciences-based data analysis).
- Are generally confined to very specific industry segments and use cases, for example, insurance, finance, project management, etc.
- Do not provide the rich flexibility of the author's approach for textbook teaching with Java applications.

Miscellaneous:

Note that IEEE, IEE, Informs, libraries of all academic institutions, IT companies, USAF, and DHS, to name a few, can be inferred as potential readers of this book.